**LAB NO. 08**

**WIRESHARK LAB: DNS** ****

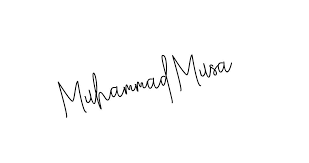
**DATA COMMUNICATION AND COMPUTER NETWORKS LAB**

Submitted by:

Name : **Muhammad Musa**

Reg no**. : 22PWCSE2157**

ClassSection **: C**



Student Signature: \_\_\_\_\_\_\_\_\_\_\_\_

Date: June 01 2025

**Submitted to:** **Dr. Yasir Saleem Afridi**

**Department of Computer Systems Engineering**

**University of Engineering and Technology, Peshawar**

**CSE 303L: Data Communication and Computer Networks**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Demonstration of Concepts** | **Poor (Does not meet expectation (1))**  The student failed to demonstrate a clear understanding of the assignment concepts | **Fair (Meet Expectation (2-3))**  The student demonstrated a clear understanding of some of the assignment concepts | **Good (Exceeds Expectation (4-5)**  The student demonstrated a clear understanding of the assignment concepts | **Score**  **30%** |
| **Accuracy** | The student mis-configured enough network settings that the lab computer couldn't function properly on the network | The student configured enough network settings that the lab computer partially functioned on the network | The student configured the network settings that the lab computer fully functioned on the network | **30%** |
| **Following Directions** | The student clearly failed to follow the verbal and written instructions to successfully complete the lab | The student failed to follow the some of the verbal and written instructions to successfully complete all requirements of the lab | The student followed the verbal and written instructions to successfully complete requirements of the lab | **20%** |
| **Time Utilization** | The student failed to complete even part of the lab in the allotted amount of time | The student failed to complete the entire lab in the allotted amount of time | The student completed the lab in its entirety in the allotted amount of time | **20%** |

**Credit Hours: 1**

# LAB 08 WIRESHARK LAB: DNS

**The Domain Name System (DNS)** translates hostnames to IP addresses, fulfilling a critical role in the Internet infrastructure. In this lab, we’ll take a closer look at the client side of DNS. Recall that the client’s role in the DNS is relatively simple – a client sends a query to its local DNS server, and receives a response back.

The hierarchical DNS servers communicate with each other to either recursively or iteratively resolve the client’s DNS query. From the DNS client’s standpoint, however, the protocol is quite simple – a query is formulated to the local DNS server and a response is received from that server.

**Tracing DNS with Wireshark**

* Open Wireshark and enter “ip.addr == your\_IP\_address” into the filter, whereyou obtain your\_IP\_address with ipconfig. This filter removes all packets thatneither originate nor are destined to your host.
* Start packet capture in Wireshark.
* With your browser, visit the Web page: http://www.ietf.org
* Stop packet capture.

To print a packet, use File->Print, choose Selected packet only, choose Packet summary line, and select the minimum amount of packet detail that you need to answer the question.

1. Locate the DNS query and response messages. Are then sent over UDP or TCP?

* The DNS query and response messages are sent over UDP.

1. What is the destination port for the DNS query message? What is the source port

of DNS response message?

* Destination Port of DNS Query: 53
* Source Port of DNS Response: 51593

1. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

* The DNS query is sent to the IP address 192.168.100.177.
* Yes, the IP addresses are same

1. Examine the DNS query message. What “Type” of DNS query is it? Does the

query message contains any “answers”?

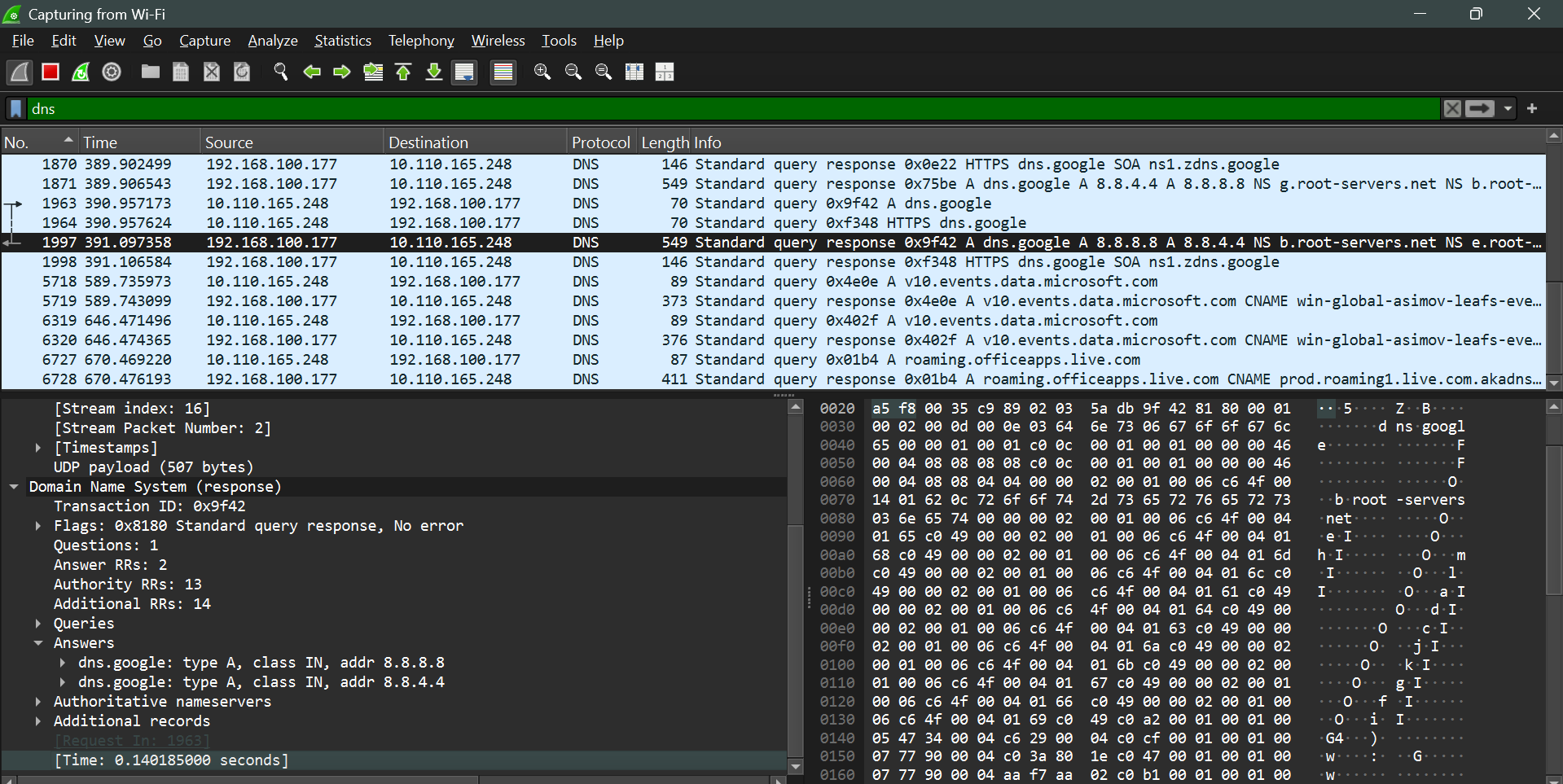
* The Type of DNS query is Type A
* Yes, the DNS query message contains answers

1. Examine the DNS response message. How many “answers” are provided? What

do each of these answers contain?

* There are 2 Answer Resource Records, indicating that the query was resolved with two valid responses:
* **Answer 1**:
  + Name: dns.google
  + Type: A (IPv4 address record)
  + Class: IN (Internet)
  + Address: 8.8.8.8
* Answer2:
  + Name: dns.google
  + Type: A (IPv4 address record)
  + Class: IN (Internet)
  + Address: 8.8.4.4

These two are the public DNS servers provided by Google.



**nslookup:**

Now let’s play with *nslookup*.

• Start packet capture.

• Do an *nslookup* on www.mit.edu

• Stop packet capture.

You should get a trace that looks something like the following:

A screenshot of a computer

AI-generated content may be incorrect.

We see from the above screenshot that *nslookup* actually sent three DNS queries and received three DNS responses. For the purpose of this assignment, in answering the following questions, ignore the first two sets of queries/responses, as they are specific to *nslookup* and are not normally generated by standard Internet applications. You should instead focus on the last query and response messages.

1. What is the destination port for the DNS query message? What is the source port of DNS response message?
   * Destination Port is 59760
   * Source Port is 53
2. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

* The DNS query is sent to the IP address 192.168.100.177
* Yes, the IP addresses are same

1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

* Type of DNS query: Type A
* Yes it contains answers**.**

1. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

* It contains 3 answers
* The answer contains the domain name being queried, type, class and address

1. Provide a screenshot.

